The Honorable Ricardo S. Martinez

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. ANDRII KOLPAKOV, Defendant.	NO. CR18-159RSM **UNITED STATES' SENTENCING MEMORANDUM**

The United States of America, by and through undersigned counsel, files this Memorandum in anticipation of the sentencing hearing in this matter. Sentencing is scheduled for June 24, 2021, to be held by videoconference with the defendant's consent.

I. INTRODUCTION

Defendant Andrii Kolpakov was a key member of the notorious transnational hacking group commonly referred to as "FIN7." FIN7 was one of the top cybersecurity threats for companies in the retail, restaurant, and hospitality industries and other such consumer-facing businesses that used point-of-sale (or "POS") terminals to process payment card transactions. For this reason, cybersecurity experts have described FIN7 as

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

"one of the most prolific financial threat groups of this decade."[1] The scope of the harm caused by FIN7 is staggering: FIN7 targeted and attacked hundreds of U.S. businesses, stole tens of millions of payment cards, and – by some estimates – caused over a billion dollars of damage.

Defendant Kolpakov appears before the Court after pleading guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking, charged in Counts 1 and 16, respectively. Defendant served as a high-level hacker and a manager of a hacker team for FIN7. In that capacity, he played a vital role in breaching the networks of countless companies and compromising millions of payment cards. And, Defendant did so, knowing the illegality and disproportionately immense harm, for over two years until his arrest in June 2019 on charges filed in this district.

For the reasons set forth below and in the government's related filing, the United States joins in the recommendation of the U.S. Probation Office and respectfully recommends that the Court impose a sentence of ***84 months***. The United States further requests the Court order restitution and forfeiture, as discussed below.

II. FACTUAL BACKGROUND

A. The FIN7 Criminal Enterprise

Cybercrime has evolved dramatically in the last decade.[2] What was once the province of lone wolf hackers, became a crowded space filled with financially motivated hacking crews led by charismatic hackers such as Roman Seleznev and David Schrooten, who were sentenced in this district to 27 and 14 years, respectively. At the peak of their exploits, Seleznev and Schrooten were viewed as pioneers in their field, with Seleznev's crew gaining particular notoriety for selling information for millions of stolen payment cards. In the modern age of cybercrime, these early pioneers have been overtaken by the

[1] https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html (last checked 6/16/2021).

[2] *See generally* Jonathan Lusthaus, Industry of Anonymity: Inside the Business of Cybercrime (2018).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

next wave of cybercriminals who have brought with them lessons learned from the startup explosion in the business world on how small firms can leverage technology to operate on a massive scale. As a result, rogue actors and loosely affiliated groups of hackers have now been surpassed by sophisticated cybercriminal enterprises that rely on specialization, division of labor, and cyclical malware development to take on the cybersecurity of major businesses.

No hacking group epitomizes the industrialization of cybercrime better than the FIN7 criminal enterprise. FIN7 has had over 70 members who were organized into discrete departments and teams. *See* Presentence Report ("PSR"), ¶12; Plea Agreement ("PA"), ¶11.b. One department developed a full suite of malware tools, while another department designed and sent phishing emails. Yet another department consisted of teams of hackers who surveilled and exploited victim companies that inadvertently had activated malware in the phishing emails. PSR, ¶12. FIN7 even used common project management software to direct workflow and to coordinate the efforts of its distributed workforce. PSR, ¶¶12, 30. This high level of sophistication and organization allowed FIN7 to continuously update not only its malware tools, but also its cutting-edge attack methodologies, in a manner that made FIN7 an increasingly formidable threat to even the most robust cybersecurity systems. As one cybersecurity company has explained, "FIN7 has demonstrated that they are highly adaptable, evading detection mechanisms while impacting a number of large US retail companies over an extended period of time."[3]

Since approximately August 2015, FIN7 has leveraged its workforce and its malware tools to relentlessly launch waves of attacks against hundreds of companies. PA, ¶11.b. FIN7's top-level leadership and managers made sure to extract value from every tool and employee at their disposal. Unable to match the sophistication and sheer

[3] Footprints of FIN7: Pushing New Techniques to Evade Detection, https://www.icebrg.io/blog/old-dog-new-tricks-fin7-pushing-new-techniques-to-evade-detection (last checked 6/16/2021).

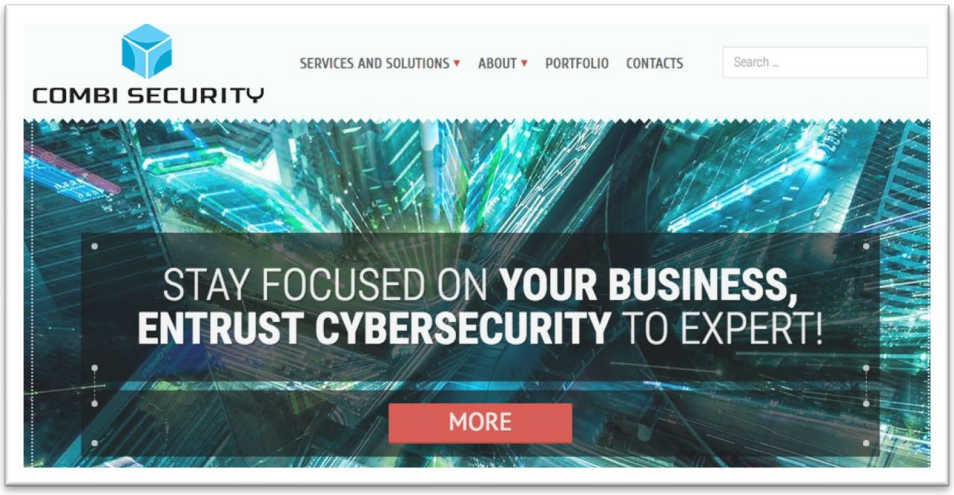
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

manpower of FIN7, numerous restaurant chains, hotels, casinos, car dealerships, law firms, and many others, were breached by FIN7's teams of hackers. PSR, ¶8.

B. Combi Security

Not only did FIN7 imitate the practices of the business world, it also masqueraded as a legitimate company. Almost comically, FIN7 created a fake cybersecurity business called "Combi Security" to, among other things, recruit and provide low-level members with plausible deniability regarding their involvement in an international hacking scheme. PSR, ¶¶9-10. Technologically skilled individuals, such as Defendant Kolpakov, were initially hired by Combi Security and may claim to believe that they thought they were joining a legitimate company. However, anyone performing any meaningful amount of work for Combi Security would have quickly realized that the company was a sham and actually a cybercriminal enterprise determined to exploit, rather than protect, the cybersecurity of its victims.

For a brief period, FIN7 even maintained a public website for Combi Security. PSR, ¶10. The website, which itself exhibited the hallmarks of a sham, stated that the company provided cybersecurity services such as penetration testing:[4]



[4] Further confirming the readily apparent illegitimacy of Combi Security, the website became inactive during the scheme. Moreover, at various points, FIN7 used different sham company names in a similar manner.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The website also claimed that:

- Combi Security was "one of the leading international companies in the field of information security";
- Combi Security had "a team of top professionals in the field of information security for all kinds of organizations working around the world."; and
- Combi Security's "main mission is to ensure the safety of your activities, minimizing the risk of information technologies. Each call to us for help, we consider very carefully on an individual basis . . ."

To add insult to injury, Combi Security's website included a "portfolio" of purported clients that had the logos of multiple victim companies. Needless to say, there is no evidence that Combi Security performed any legitimate work. PA, ¶11.d. And, surely, none of FIN7's victims hired Combi Security to "test" their security.

C. FIN7's Attack Methodology

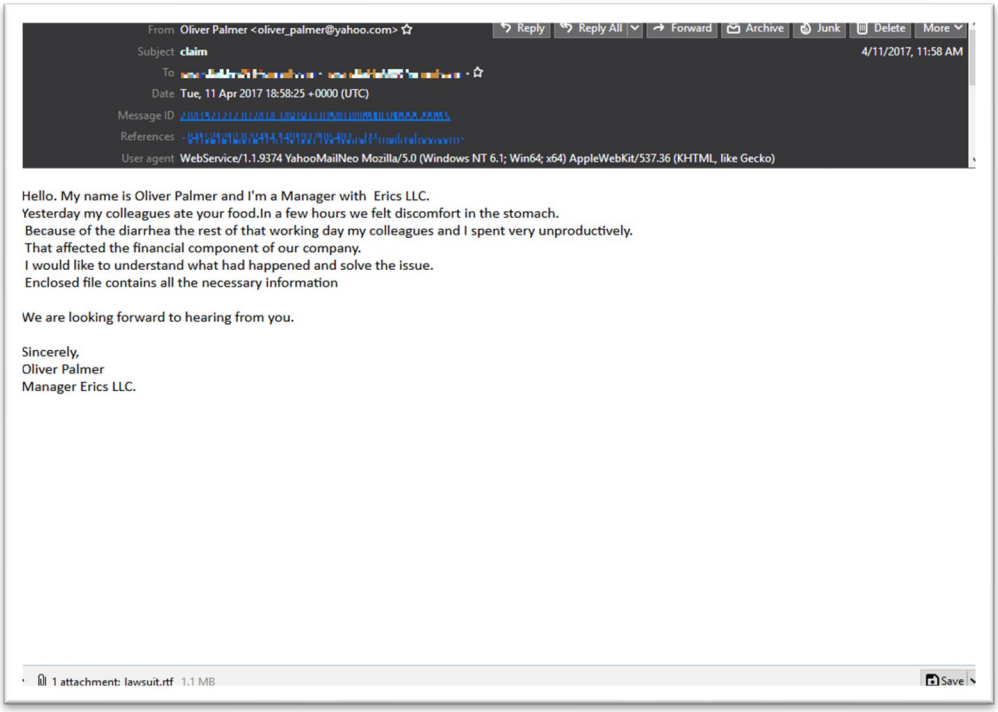
FIN7 typically attacked the weakest element of a company's cybersecurity – the human element. After conducting research on a target company, FIN7 would launch tailored phishing email campaigns against employees of the target company.[5] PSR, ¶16. Although FIN7 has sent phishing emails to employees in a variety of roles, FIN7 is well-known for targeting customer service representatives with emails that exploit the representatives' desire to be responsive to their customers.

FIN7 used a wide variety of phishing emails, some of better quality than others. For example, FIN7 sent emails to restaurant managers, such as the following,[6] that complained about getting food poisoning and exploited public health and safety concerns:

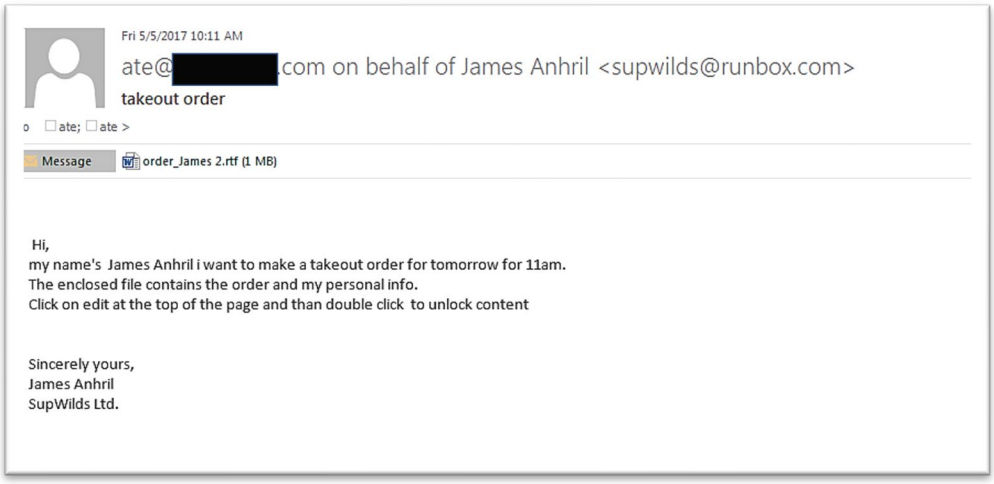
[5] *See generally* Operation Grand Mars: Defending Against Carbanak Cyber Attacks, https://www2.trustwave.com/Operation-Grand-Mars.html (last checked 6/16/2021).

[6] Victim information has been blurred or redacted in the examples contained in this memorandum.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

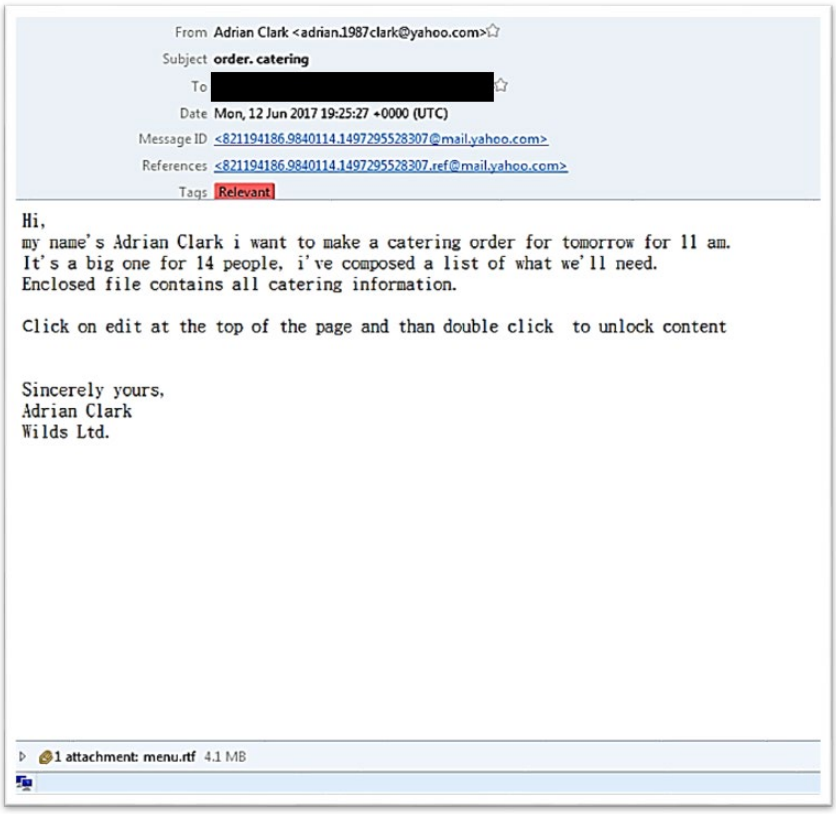


Other emails enticed the recipient to open an attachment purportedly containing a large order:



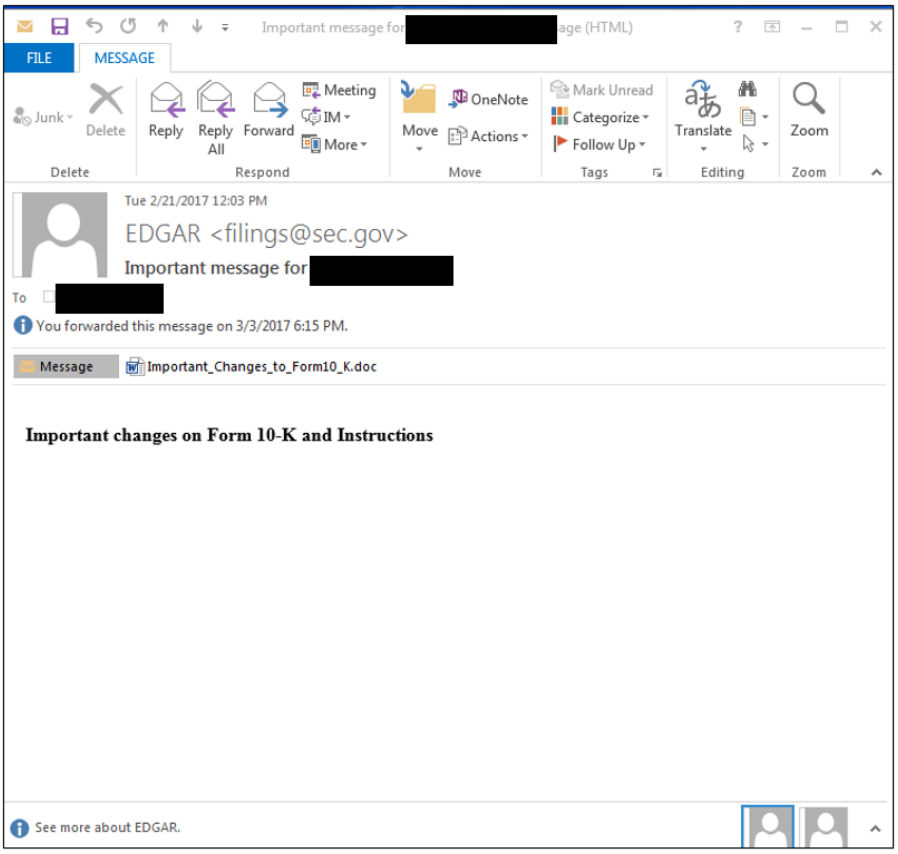
****

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



FIN7 also launched phishing attacks aimed at personnel at victim companies who had unique access to proprietary and non-public information. PSR, ¶18. For example, FIN7 targeted employees involved with preparing corporate filings with the United States Securities and Exchange Commission ("SEC"). *Id.* These emails used an email address that spoofed an address associated with the SEC's electronic filing system and induced the recipient to open an attachment to the email. The example below was delivered directly to an in-house corporate counsel of a publicly traded corporation, who was responsible for the company's securities filings:

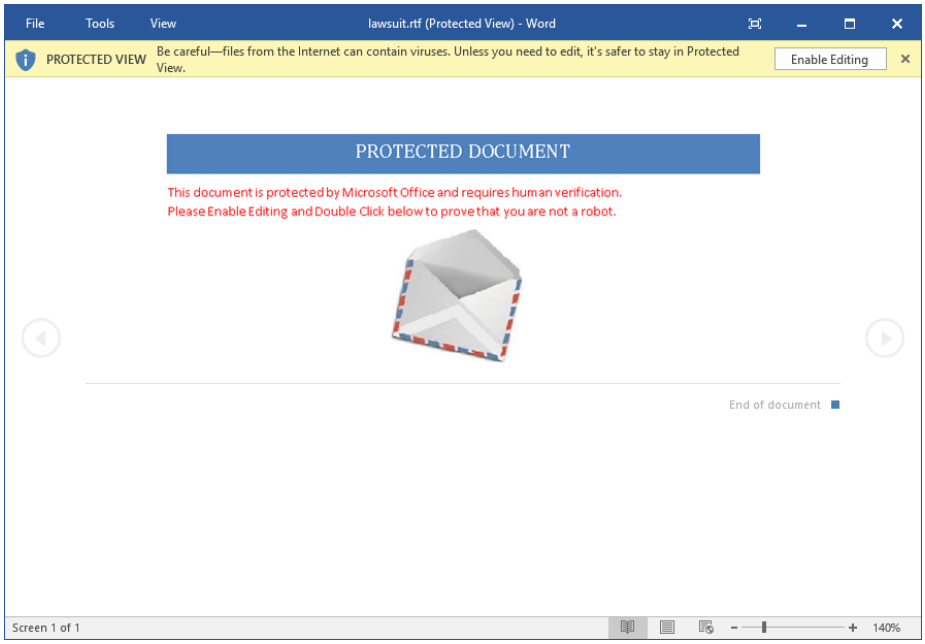
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



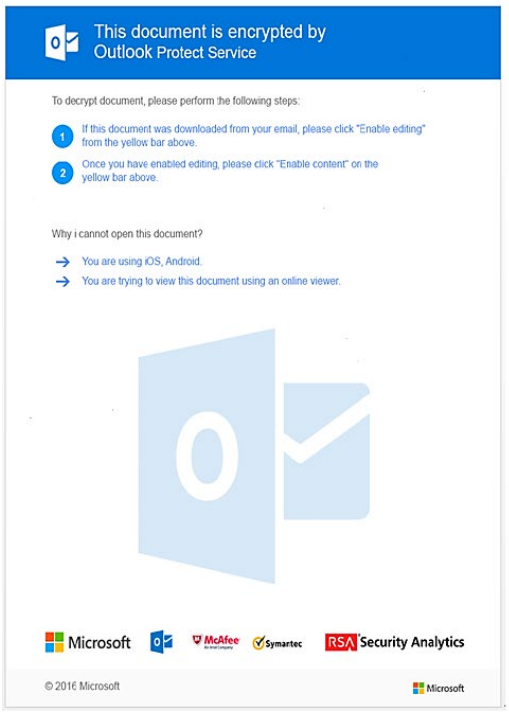
Induced by the seemingly legitimate email and the significance of the purported subject, the attorney unknowingly activated the malware and exposed the business' network to FIN7's hackers.

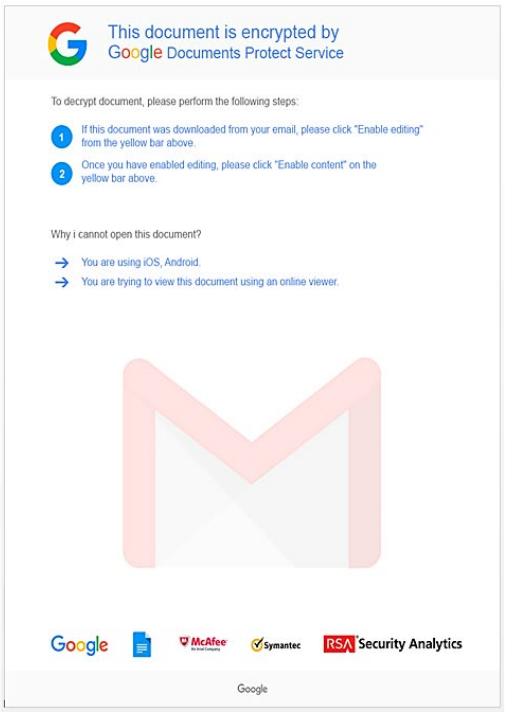
In many of the attacks, a FIN7 member, or someone hired by FIN7, also called the recipients of phishing emails and used social engineering techniques to encourage recipients to first read the emails and then open the email attachments in a manner that inadvertently activated malware embedded in the attachment. PSR, ¶19. The attachments to the phishing emails started off as rudimentary (but highly effective) Microsoft Word documents or Rich Text Format (.rtf) files with embedded malware:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



PSR, ¶17. Over time, the attachments became more and more sophisticated. Among other things, FIN7 improved the graphics in the file and incorporated trustmarks of well-known companies to increase the likelihood that recipients would activate the embedded malware, as exhibited in the examples below:





UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

FIN7 used multiple malware delivery mechanisms in its phishing attachments including, but not limited to, weaponized Microsoft Word macros, malicious Object Linking and Embedding (OLE) objects, malicious visual basic scripts or JavaScript, and malicious embedded shortcut files (LNK files).[7] PSR ¶17.

D. The FIN7 Botnet

Once the initial malware was activated, FIN7 gained a beachhead in the victim's network. PSR, ¶20. From this beachhead, FIN7 could deploy additional malware, conduct reconnaissance, and target systems that contained sensitive financial information. PA, ¶11.e. FIN7 typically used the Carbanak malware as a "backdoor" that allowed the enterprise to maintain persistent and discrete access to the victim company's network. PSR, ¶21. The Carbanak malware has robust data-stealing capabilities and even enables hackers to record activity occurring on the desktops of infected computers. In addition to the Carbanak malware, FIN7 had an arsenal of tools it used to maintain its presence in networks and to steal data. Examples of these tools include Cobalt Strike, DRIFTPIN, HALFBAKED, GRIFFON, Bateleur, and Metasploit Pro. PSR, ¶¶22-23.

FIN7's malware connected infected computers to a network of command and control servers located around the world. PSR, ¶¶20-21. FIN7 regularly incorporated compromised computers or "bots" into a "botnet" that could be controlled through custom administrative control panels. PSR, ¶¶21-22. The control panels gave FIN7 the ability to view, edit, and send commands to a particular bot. PSR, ¶22. The panels also provide an effective means for the group to receive data back from the compromised computers. PSR, ¶23. And, most importantly, perhaps, the panels provided a scalable

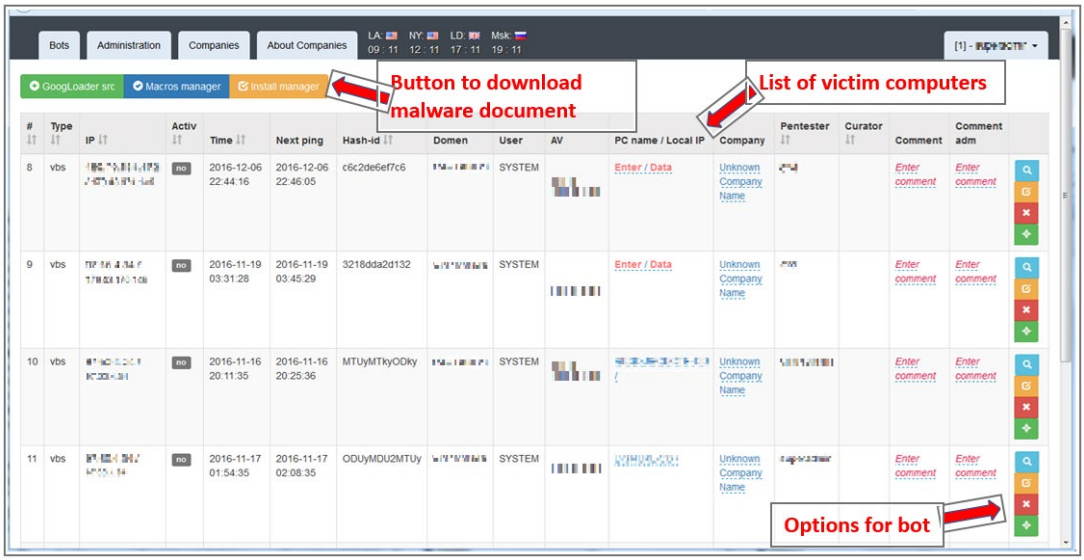
---

[7] *See* FIN7 Evolution and the Phishing LNK, https://www.fireeye.com/blog/threat-research/2017/04/fin7-phishing-lnk.html (last checked 6/16/2021); Footprints of FIN7: Pushing New Techniques to Evade Detection, https://www.icebrg.io/blog/old-dog-new-tricks-fin7-pushing-new-techniques-to-evade-detection (last checked 6/16/2021).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

way for the enterprise to not only give new members access to breached computers, but also to add an unlimited number bots to the botnet.

The custom user interface for the administrative control panel gave FIN7 convenient access and control over individual bots. The panel listed each bot and provided information, such as the PC name of the bot, domain of the bot, and whether the bot had antivirus software. When a FIN7 member selected an individual bot, the panel allowed them to run a variety of commands, such as generating a list of processes running on the bot, executing programs, and taking a screenshot. The following annotated screenshot shows a version of the control panel and illustrates the functionality of the panel's interface:



In most cases, FIN7 members were tasked with locating and compromising the victims' point-of-sale systems, in order to scrape and steal the financial data of ordinary consumers. According to a study of a sample of just fifteen million payment cards stolen by FIN7, recovered by U.S. authorities, FIN7's hackers were able to locate and exploit the point-of-sale systems of over 3,600 physical locations across the country. PSR, ¶34.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

E. FIN7's Victims

Hundreds of victim companies were attacked by FIN7. PA, ¶11.b; PSR, ¶16. These attacks resulted in the theft of troves of financial information, including the exfiltration of information for tens of millions of payment card numbers.[8] PA, ¶11.c; PSR, ¶25. The breaches and the subsequent fraudulent use of the stolen financial information impacted numerous victims including companies who were breached, financial institutions, card brands, merchant processers, insurance companies, retail companies, and individual card holders. PA, ¶11.k; PSR, ¶24.

These victims incurred enormous costs that, according to some estimates, exceeded one billion dollars.[9] The breached companies faced costs associated with remediating the breach, customer notification, lost business, resolving ensuing class action lawsuits, and potentially paying fines to state Attorney Generals and government agencies.[10] PA, ¶11.k; PSR, ¶24. The financial institutions that issued the payment cards faced losses associated with the fraudulent purchases and replacing customers' cards. Much of those losses were, in turn, passed onto businesses at which the stolen payment card numbers were used to make purchases.

FIN7 monetized the stolen financial information in various ways. One central way the enterprise sold payment card information was to advertise the sale of "dumps" of the information on underground vending sites such as Joker's Stash. PSR, ¶25. The following screenshot shows an advertisement on Joker's Stash of a dump of four million card numbers stolen by FIN7:

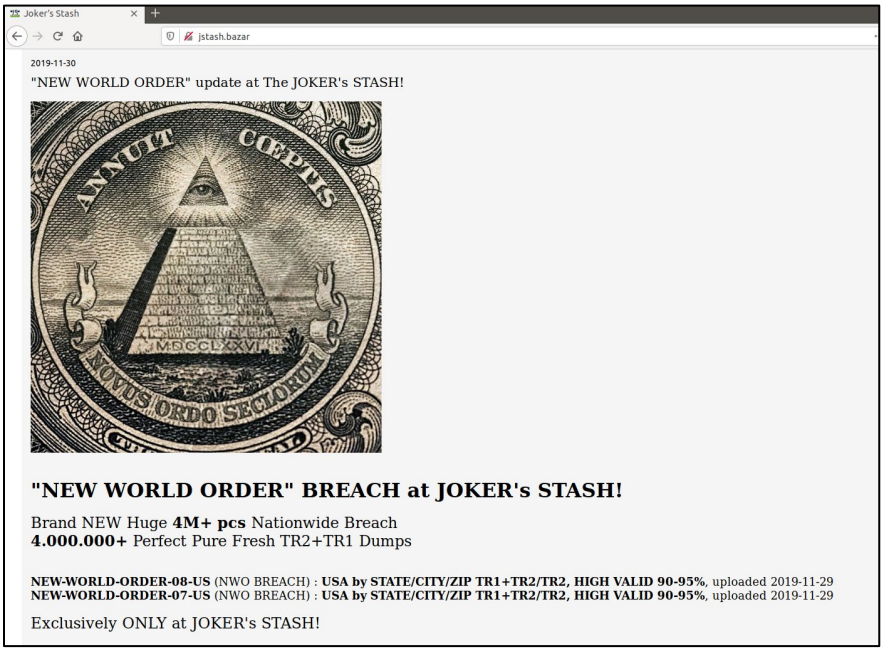
---

[8] The total number of payment cards that FIN7 stole is not at issue. For the purposes of sentencing, the parties have stipulated that Defendant Kolpakov should be held accountable for the theft of 20 million payment cards. PA, ¶12.b.

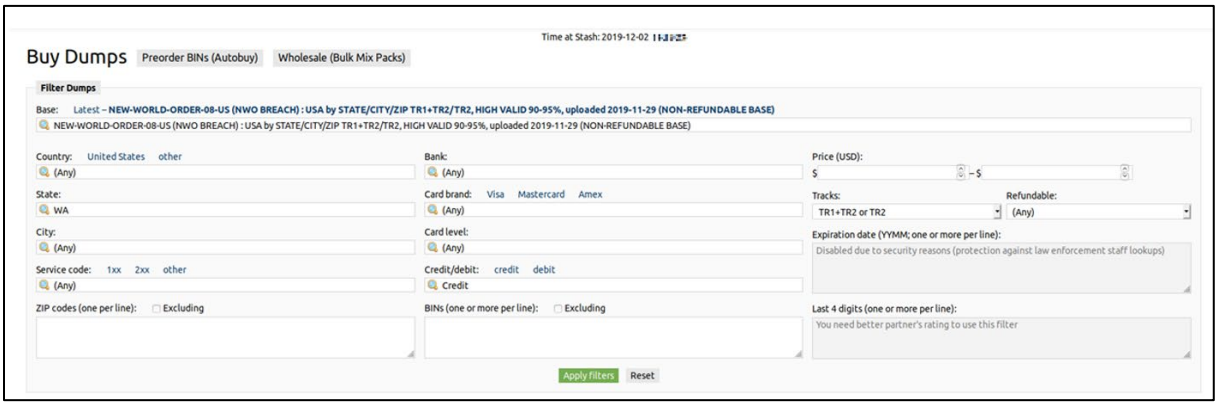
[9] The actual loss number is not at issue. The parties have stipulated that – during Defendant Kolpakov's participation in the criminal enterprise – FIN7 caused over $100 million in losses. PA, ¶11.k.

[10] The Ponemon Institute and IBM Security estimate that the average cost of a significant data breach in the United States in 2020 was **$8.64 million**. *See* https://www.ibm.com/security/data-breach (last checked 6/16/2021).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970



As shown in the next screenshot, Joker Stash allowed fraudsters to sort through solen payment cards by the type of card stolen (debit or credit), the level of the card (classic or platinum), and the state in which the owner of the card resided:



Fraudsters who purchased the stolen information would then imprint the information on blank payment cards so they could be used to conduct fraudulent purchases. The location of the legitimate card holder assists fraudsters in avoiding fraud alerts and detection mechanisms designed to notify financial institutions when customer cards are used to make purchases outside of the card holder's state of residence.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

F. Defendant's Role as a FIN7 Hacker and Team Leader

From at least April 2016 to his arrest on June 28, 2018, Defendant Kolpakov served as a high-level hacker, whom FIN7 referred to internally as "pentesters," and was directly involved in breaching the networks of numerous prominent U.S. businesses. In that role, he probed and mapped victims' networks in search of point-of-sale systems and customer payment card data. For instance, Defendant substantially participated in the hack of Jason's Deli ("Victim-6"), a U.S.-based delicatessen restaurant chain with hundreds of locations, from which millions of customer records were stolen and ultimately sold on the dark web. PSR, ¶29.

Defendant's technical acumen allowed him to rise within the enterprise. He was elevated to a managerial role in which he also managed and supervised a small team of hackers tasked with breaching the security of victims' computer systems. PA, ¶11.g. He was assigned to supervise and train new recruits and apprised his team members of new tools and developments in the FIN7's phishing campaigns and malware arsenal. PA, ¶11.h. Defendant might be described as a mid-level manager or team leader.

During the course of the scheme, Defendant received compensation for his participation in FIN7, which far exceeded comparable legitimate employment available in Ukraine. For the purposes of this sentencing, the parties agree and stipulate that the compensation was approximately $75,000 (USD). By comparison, and highlighting the disproportionate harm caused by hacking, during Defendant's participation in the malware scheme – FIN7 illegal activity resulted in over $100 million in losses to financial institutions, merchant processers, insurance companies, retail companies, and individual cardholders.

While Defendant was working for FIN7, a number of companies, including Jason's Deli (Victim-6), publicly reported that they had suffered data breaches involving the theft of payment card information that were later attributed to FIN7. Moreover, Defendant Kolpakov and his associates received reports of arrests of other FIN7

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

members, including Fedir Hladyr and Dmytro Fedorov. Defendant nevertheless continued as part of the criminal enterprise attacking businesses in the United States and elsewhere.

On about June 28, 2018, Defendant Kolpakov was arrested by Spanish police while on vacation in Lepe, Spain, based on charges from this federal district. At the time, he was in possession of electronic devices, including an Asus laptop computer (with hard drives), storage devices, and a mobile phone, described below, which were used to facilitate the scheme. For instance, on those devices, Defendant knowingly possessed, among other things, multiple thousands of payment card numbers and employee credential information stolen from various U.S. victim companies through the aforementioned hacking activity on behalf of the FIN7 hacking group. Upon Defendant's arrest by Spanish police, Defendant's travel companion sent a message to another FIN7 member also traveling in Spain to advise of the arrest.

III. PLEA AGREEMENT AND SENTENCING GUIDELINES

Defendant Kolpakov was extradited by Spain to the United States, and he made his initial appearance in this federal district on June 3, 2019. He was ordered detained and has remained in custody since his initial arrest.

A. The Plea Agreement

On November 16, 2020, Defendant Kolpakov entered guilty pleas to one count of Conspiracy to Commit Wire Fraud (Count 1), in violation of 18 U.S.C. § 1349, and one count of Conspiracy to Commit Computer Hacking (Count 16) in violation of 18 U.S.C. § 371. PA, ¶1 (Dkt. #48). The plea agreement includes an extensive statement of facts setting forth a summary of Defendant Kolpakov's role as a high-level hacker and manager of other hackers tasked with breaching the security of victims' computer systems. *See* PA, ¶11.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

1. Dismissal of Remaining Counts

Pursuant to Paragraph 1 of the plea agreement, the United States requests dismissal of Counts 2-15 and 17-26 of the Indictment at the time of sentencing.

2. Forfeiture

Defendant stipulated that he received compensation for his participation in FIN7, which far exceeded comparable legitimate employment in Ukraine. *See* PA, ¶11.k. Consistent with that stipulation, Defendant agreed in Paragraph 9 of the plea agreement to forfeit a sum of money in the estimated amount of proceeds that Defendant obtained as a result of the offense set forth in Count 1. Defendant further agreed to forfeit his rights and interests in several digital devices seized by law enforcement, which were used to facilitate the commission of the offense, namely:

a. Asus laptop, model no. X510U (serial no. HANOCX24R525436);

b. Toshiba 128 GB SSD (serial no. 671510BATMXT);

c. SATA hard drive (serial no. 87VEC1G9T SWF HDKCB8888E0A01T);

d. Gold colored Samsung SM J500H Galaxy J5 cell phone (serial no. RV1H40M03WV, IMEI 357950071755024/01 and 35800071755027/0); and

e. Various SIM cards.

On June 10, 2021, the United States filed a Stipulated Motion for Entry of a Preliminary Order of Forfeiture, which requested forfeiture of the above-listed devices and a sum of money in the amount of $75,000. Dkt. #53. The United States respectfully requests that the Court grant the stipulated motion and incorporate the order as part of Defendant's sentence imposed at the sentencing hearing.

3. Restitution

The harm caused by Defendant and his FIN7 co-conspirators is enormous. For the purposes of sentencing, the parties have stipulated that the actual loss to financial institutions, merchant processers, insurance companies, retail companies, and individual cardholders during Defendant's involvement in the enterprise exceeded $100 million.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

See PA, ¶11.k. In Paragraph 8 of the plea agreement, Defendant agreed to pay restitution in the apportioned amount of $2,500,000. Accordingly, the United States requests that the Court enter a restitution judgment in this amount, apportioned to victims as set forth in the presentence report (PSR, ¶106), and specify that this obligation shall not be joint and several with any other FIN7 defendant.

4. Appellate Wavier

In paragraph 16 of the plea agreement, Defendant waived his appellate rights and his rights to collateral attack provided that the Court imposes a custodial sentence that is within or below the Sentencing Guidelines range. Assuming the Court imposes a term of incarceration that is within or below the Sentencing Guidelines range as determined by the Court at the time of sentencing, the United States requests that the Court advise Defendant appropriately regarding his remaining appellate rights, following imposition of sentence.

B. The Presentence Report and the Offense Level Calculation

In Paragraph 12 of the plea agreement, the parties stipulated to the following Guidelines calculation:

a. A base offense level of 6, pursuant to USSG § 2B1.1(a)(2).

b. An offense level enhancement of 30 levels (+30), based on a loss amount of more than $550,000,000, pursuant to USSG § 2B1.1(b)(1)(P). For the purposes of this plea agreement, the parties agree to limit the number of stolen payment cards to 20 million, which represents the approximate number of unique card numbers recovered to date. Pursuant to Application Note 3(F)(i), a $500 loss amount is imputed to each payment card, resulting in a total loss amount, for Guidelines purposes, of $10 billion.

c. An offense level enhancement of 2 levels (+2), because the offense involved more than 10 victims, pursuant to USSG § 2B1.1(b)(2)(A).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. An offense level enhancement of 2 levels (+2), because the offense involved receiving stolen property, and the defendant was a person in the business of receiving and selling stolen property, pursuant to USSG § 2B1.1(b)(4).

e. An offense level enhancement of 2 levels (+2), because a substantial part of the fraudulent scheme was committed from outside the United States and because the offense involved sophisticated means and the defendant intentionally engaged in and caused the conduct constituting sophisticated means, pursuant to USSG § 2B1.1(b)(10).

f. An offense level enhancement of 2 levels (+2), because the offense involved the trafficking in unauthorized access devices and counterfeit access devices and because the offense involved the possession of more than 5 means of identification that were unlawfully obtained, pursuant to USSG § 2B1.1(b)(11).

g. An offense level enhancement of 3 levels (+3), because the defendant was a manager (but not an organizer or leader) and the criminal activity involved more than five participants and was extensive, pursuant to USSG § 3B1.1(b).

h. An offense level reduction for acceptance of responsibility, pursuant to USSG § 3E1.1.

The stipulated Guidelines provisions result in a total offense level of 43, the maximum allowable, after crediting Defendant with a three-point reduction (3) for timely acceptance of responsibility. Defendant Kolpakov falls within criminal history category I, as he has no countable criminal convictions.

The United States Probation Office prepared a final presentence report on June 10, 2021 with a Guidelines calculation that is consistent with the parties' stipulations. A total offense level of 43, even coupled with a criminal history category I, would result in an advisory sentence of *life* under the Guidelines. However, in this case, the Guidelines range of imprisonment is the statutory maximum sentence of 25 years, pursuant to USSG § 5G1.1.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

C. Defendant's Time in Custody

It is the government's understanding that the Bureau of Prisons will give Defendant Kolpakov credit for the time he has spent in law enforcement custody since his initial arrest in Spain on June 28, 2018. PSR, ¶5. At the time of the sentencing hearing on June 24, 2021, Defendant will have been in law enforcement custody for approximately 36 months.

IV. SENTENCING RECOMMENDATION

The United States joins the Probation Office and recommends a custodial sentence of ***84 months*** for Defendant Kolpakov --- specifically, 84 months for Count 1 and 60 months for Count 16, to be served concurrently. The United States further joins in recommending a three-year term of supervised release and a $2,500,000 restitution obligation. As discussed below, the United States submits that this recommended sentence is sufficient but not greater than necessary, and is justified by a balancing the factors set forth in Title 18, United States Code, Section 3553(a).

As the Ninth Circuit and the Supreme Court have explained, the Sentencing Guidelines are "the 'starting point and the initial benchmark' . . . and are to be kept in mind throughout the process." *United States v. Carty*, 520 F.3d 984, 996 (9th Cir. 2008) (internal citations omitted). Title 18, United States Code, Section 3553(a), sets forth factors for the Court to consider alongside the advisory Guidelines range. The United States submits that the recommended sentence is appropriate particularly in light of "the nature and circumstances of the offense," "the history and characteristics of the defendant," and the need for the sentence "to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense," "to afford adequate deterrence to criminal conduct," and "to avoid unwarranted sentence disparities." 18 U.S.C. §§ 3553(a)(1), (a)(2), and (a)(6).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A. The Nature and Circumstances of the Offenses

The nature and circumstances of Defendant Kolpakov's offenses are unprecedented in this district. Defendant was an active and significant member of one of the most sophisticated and successful hacking groups in modern times. Under the advisory Guidelines, Defendant is accountable for a loss amount of $10,000,000,000. *See* USSG § 2B1.1(b)(1), Application Note 3(F)(i). No defendant in memory has been accountable for a larger loss amount in this district.

Although the aggregate loss amount under the Guidelines is astronomical, it does not adequately convey the actual harm that Defendant and his FIN7 co-conspirators caused to victims around the world. FIN7 was relentless in its repeated attacks against hundreds of companies. As explained in Section II.E, *supra*, these attacks negatively impacted numerous parties including the companies whose security was breached, the card brands and financial institutions associated with the stolen payment cards, the individual card holders who had their information stolen, and the businesses at which the stolen payment cards were later used to make fraudulent purchasers. Defendant Kolpakov deserves a sentence that recognizes the enormity of the harm he and his cohorts caused to these victims.

The scale and sophistication of the FIN7 criminal enterprise is also an aggravating factor. Unlike groups of rogue cybercriminal actors, FIN7 approached hacking with the premeditated discipline and refinement of a multinational business operation, which it essentially was, albeit with an illegal and nefarious business plan. FIN7's structure assigned discrete aspects of the hacking and monetization processes across members and groups, all subject to a management hierarchy comprised of managers and top-level bosses, who operated like executives. For instance, while certain members continued to develop and improve the phishing email messaging and social engineering techniques, others continued to build upon the enterprise's suite of malware tools. Others managed the physical infrastructure of the operation, while also providing mentorship and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

technical training to subordinates. Only a complex and disciplined enterprise like FIN7 could have integrated these diverse roles in a cohesive and scalable manner that allowed the enterprise to have a devastating worldwide impact.

Defendant Kolpakov substantially contributed to FIN7's nefarious mission, having worked for the group for over two years, from roughly April 2016 to June 28, 2018. Moreover, despite growing news of the significance of FIN7's hacks and reports of colleagues' arrest, Defendant persisted, drawn by the financial rewards and the belief that those illegal profits far outweighed the risk or severity of punishment. Indeed, only Defendant's arrest by foreign officials, at the request of U.S. authorities, stopped his involvement in this unprecedented criminal enterprise.

That said, Defendant Kolpakov was not a top-level member in the organization. He was aware of the criminal nature of the conduct and he managed other individuals, but he functioned as a mid-level manager, handling a team of hackers working on particular projects. Defendant did not make high-level decisions, nor was he among those who engineered the scheme or collected the majority of the organization's profits. The Probation Office's and the government's recommendation, well below the advisory range, acknowledges and incorporates this factor.

Defendant Kolpakov may attempt to distance himself from the astonishing losses and harms caused by citing his limited role and/or the actual proceeds he received personally. However, a sophisticated cybercriminal like Defendant Kolpakov should not be permitted to raise disproportionality as a shield for at least three central reasons.

First, the asymmetry between the relatively limited investment of resources by cybercriminals and the enormous harm they cause is exactly what makes cybercrime so alluring. Cybercriminals like Defendant Kolpakov pose such a great threat because they use their specialized skills and training to *amplify* the reach and impact of their criminal activity. Instead of having to physically rob a thousand individual locations of a major restaurant chain one-by-one, FIN7 hackers were able to deploy a single methodology to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

rob thousands of locations of multiple restaurant chains simultaneously from the comfort and safety of their keyboards in distant countries. Moreover, given the near limitless reach, FIN7 hackers would never exhaust possible targets and victims. In short, in this illicit context, the economies of scale are extremely high. Consequently, Defendant Kolpakov cannot equitably invoke disproportionality when he made a deliberate decision to leverage his technological expertise to carry out his criminal activity on a massive scale.

Second, and relatedly, the asymmetrical harm caused by Defendant's offenses were the foreseeable and intended consequences. This is not a case where a defendant takes a simple action that cascades into a series of unpredictable events. To the contrary, Defendant Kolpakov and his co-conspirators knew exactly what they were doing and the harm that they would cause. FIN7's methodology relied on volume – to hack and harvest the maximum amount of financial data, and in turn to indiscriminately impact the maximum number of individual victims. Defendant and his co-conspirators fully understood the devasting harm the data breaches would cause and the large amount of fraudulent purchases that would be made with the stolen payment card information. Because this was the intended result of FIN7's relentless attacks, Defendant cannot now claim to be a victim of his own success in helping to accomplish this goal.

Third, criminal proceeds from cybercrime are almost always substantially less than the harm incurred by victims. This is particularly true when hackers attempt to profit from stolen payment card information. FIN7 monetized the stolen payment card information by selling it in bulk sales on underground forums such as Joker Stash. As a result, the proceeds that FIN7 received per stolen payment card was relatively low (compared to the ensuing fraudulent purchases made using the stolen card information), particularly after middlemen who facilitated the sales took their cut. Defendant Kolpakov cannot reasonably contend that he is entitled to a sentencing discount because

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

he received only a portion of the overall profits made by all the criminals who exploited the stolen payment card information.

B. Defendant's History and Characteristics

Defendant Kolpakov's history and characteristics provide mitigation and weigh in favor of a sentence below the advisory Guidelines range. The recommended sentence appropriately considers that Defendant has no prior criminal history, has employable skills and work history, and held legitimate jobs before he joined FIN7. The government further recognizes the unique challenges Defendant faced, and overcame, in his youth. However, the recommended sentence also considers the egregious misuse of his skills and the fact that Defendant still poses a risk of recidivism. After Defendant is released, he will be deported and likely will return to Ukraine. As the public is increasingly aware, cybercrime can be a lucrative venture, and unfortunately many countries do not pursue meaningful enforcement actions against hackers and cybercriminals. The influences that Defendant claims induced him to join FIN7 will remain when he reenters society after serving his sentence. It remains to be seen whether Defendant will resist the lure of the potential rewards by again leveraging his technical expertise to commit crime.

C. The Need for the Sentence to Reflect the Seriousness of the Offenses, to Promote Respect for the Law, and to Provide Just Punishment

These factors weigh strongly in favor of a judgment that imposes a lengthy term of incarceration. Given FIN7's notoriety, this case will be used as benchmark for sentences in other cybercrime cases, in this district and elsewhere. Crimes like those committed by Defendant Kolpakov pose serious threats to the viability of businesses and financial institutions everywhere, as well as to the security of their customers. A seven-year custodial sentence would send a message that there are harsh consequences for joining and advancing a cybercriminal enterprise like FIN7.

The need to promote respect for laws that prohibit cybercrime is particularly high given the major increase in attacks against U.S. interests that are launched by foreign

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

actors. It is unfortunately rare that a member of a sophisticated cybercriminal organization is identified, arrested, and extradited for prosecution in the United States. Too often, international cybercriminals can conceal their identities or hide in countries in which they are beyond the reach of law enforcement. Accordingly, this case presents a rare opportunity to demonstrate that not only can law enforcement identify and arrest sophisticated cybercriminals, but also that such cybercriminals face harsh consequences for attacking U.S. businesses and consumers.

Finally, no discussion of these factors would be complete without additional mention of the enormous harm that Defendant Kolpakov and his co-conspirators caused to numerous victims. These victims included, at a minimum, "financial institutions, merchant processers, insurance companies, retail companies, and individual cardholders."[11] PA, ¶11.k. A seven-year sentence is needed to provide just punishment and to vindicate the interests of these victims.

D. The Need to Afford Adequate Deterrence to Criminal Conduct

High rewards coupled with a relatively modest risk of detection and an even lower risk of apprehension are basic features of modern cybercrime. However, appropriately severe sentences can impact the cost-benefit analysis of would-be cybercriminals. Computer hackers are among the most sophisticated criminals in the world and are known to closely monitor U.S. authorities' response to cybercrime and react accordingly. Achieving general deterrence in this area, therefore, appears somewhat promising. *See United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (because "economic and

[11] It is important to note the general public bears much of the cost caused by cybercriminal enterprises. When businesses sustain fraud-related losses or expenses, they generally pass these costs on to the average American in the form of higher prices, fees and other indirect charges. *See* Lydia Segal, *Credit Card Fraud: A New Perspective on Tackling an Intransigent Problem*, 16 FORDHAM J. CORP. & FIN. L. 743, 754, 775 (2011) (banks and credit card companies pass on costs of fraud to consumers in the form of higher prices, banking costs, and other charges); *see also* Ronald Mann, *Credit Cards and Debit Cards in the United States and Japan*, 55 VAND. L. REV. 1055, 1093-94 (2002) (credit card companies pass on costs of fraud to cardholders and merchants).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

fraud-based crime are more rational, cool, and calculated than sudden crimes of passion or opportunity, these crimes are prime candidates for general deterrence").

This case demonstrates that there is an acute need to impose a sentence that deters others from joining cybercriminal organizations. Criminal enterprises such as FIN7 rely on the ability to recruit technologically skilled individuals, such as Defendant Kolpakov. A meaningful sentence will put potential recruits on notice that engaging in cybercrime will subject them to significant penalties and prison sentences that are commensurate with the harm they inflict. A meaningful sentence will likewise send a message to FIN7 members still engaged in the criminal enterprise. Intercepted communications between these members show that they are closely watching the progression of the cases against their former colleagues. It is important that they know the severe consequences they face --- not just for their past crimes, but any future crimes. Giving their valued colleagues significant jail time will convincingly convey, at least to some, that the cost of doing business is simply too high.

E. The Need to Avoid Unwarranted Sentencing Disparity

Cybercrime takes many forms, and it is difficult to compare cybercriminal schemes that utilize different methodologies and that impact different groups of victims. For this reason, it is difficult to compare sentences imposed on defendants who participated in different cybercriminal enterprises. Nevertheless, two cases from the Western District of Washington provide important reference points.

In the first case, *United States v. Schrooten*, CR12-085RSM, this Court sentenced a prominent hacker and payment card thief to 12 years pursuant to a Rule 11(c)(1)(C) plea agreement. Although Schrooten's carding ring was considered substantial at the time, he had in his possession only 100,000 stolen payment card numbers. Of note, in the *Schrooten* case, this Court imposed a seven-year sentence on a lower-level member of the carding ring who had possession of only 86,400 stolen payment cards.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In the second case, *United States v. Roman Seleznev*, CR11-70RAJ, the Honorable Richard A. Jones sentenced the leader of an extensive payment card trafficking ring to 27 years after he was convicted at trial. Seleznev's carding ring was substantially smaller in scope than FIN7, and he ultimately was held responsible for only 2.9 million stolen payment cards that were found in his possession. However, there were many aggravating factors in Seleznev's case including his leadership role, the enormous amount of proceeds he received, his extensive efforts to obstruct justice, and evidence that he had stolen many more payment cards.

The *Schrooten* and *Seleznev* cases involved schemes that were orders of magnitude smaller than the FIN7 criminal enterprise. However, both primary defendants were deserving of harsher sentences than Defendant Kolpakov because they were the leaders of their respective schemes and reaped most of the illegal proceeds. Although Defendant Kolpakov was an active and valued member of FIN7, he was not among the top leadership tier nor the driving force behind his criminal enterprise. While he supervised and managed others, he did not exercise the type or degree of authority indicative of an organizational leader. Rather, Defendant served as a skilled operative and middle manager within the hacking organization. Accordingly, in the government's view, a sentence of seven years appropriately balances the differences between these cases and achieves a just result.

Furthermore, this Court recently sentenced a co-conspirator, FIN7 member Fedir Hladyr, to ten years in prison in related case *United States v. Hladyr*, CR17-00276RSM. Hladyr, also a Ukrainian national arrested while on vacation, was a high-level manager and systems administrator for FIN7 responsible for providing technical guidance and for setting up and maintaining a worldwide network of servers used to enable and carry out cyberattacks. He likewise was recruited to Combi Security and previously had held legitimate employment. Upon appearing in this district, Hladyr also entered timely guilty pleas to the same charges pursuant to a similar plea agreement and otherwise is similarly

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

situated to Defendant Kolpakov with respect to efforts to demonstrate contrition and acceptance of responsibility.[12]

By any metric, Defendant Kolpakov held a far inferior position within the FIN7 operation. He managed and supervised a small team of hackers, with limited actual decision-making authority. While a valued and active participant, Defendant, unlike Hladyr, did not hold a key high-level position in proximity to the top-tier leaders. However, Defendant also presents aggravating factors not present in Hladyr's case. For instance, unlike the latter, Defendant Kolpakov fought extradition, which in turn absorbed government resources and substantially delayed his transfer to U.S. custody and appearance on charges in this district. That said, once extradited, Defendant immediately accepted responsibility and exhibited contrition, as described in more detail in the government's prior related filing. In light of the totality of the circumstances and various factors likening and distinguishing him from Hladyr, the government submits that imposing a seven-year sentence appropriately balances the factors of this case and would not cause an unreasonable disparity.

It is truly unfortunate that, despite employable skills and viable alternatives, Defendant Kolpakov nevertheless elected to turn to illegal hacking activity. In making that decision as well as the repeated decisions to continue along that path over the course of years, Defendant placed his financial gain over the egregious and asymmetric harm he helped inflict upon countless innocent victims. The United States sincerely hopes that Defendant Kolpakov's assurances and statements of contrition are sincere and that this

[12] As set forth in the United States' sentencing material in the related case, there was a level of leadership above Hladyr that likely received the lion's share of the criminal proceeds. In recommending a ten-year sentence, the United States weighed heavily the fact that Hladyr was not a top-level leader in the criminal enterprise and, as a result, did not make millions in profit. Although the proceeds Hladyr received were modest by Western standards, they were substantial by Ukrainian standards and allowed him to afford luxuries like a European tour and visit to Disneyland Paris. Fittingly, it was that trip that led Hladyr's arrest on his return route through Germany.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

encounter with the U.S. criminal justice system has conveyed to him, and other current and potential hackers, to steer clear of such criminal ventures going forward.

V. CONCLUSION

For the reasons set forth above and in the government related filing, the United States respectfully requests that the Court impose a total sentence of 84 months as set forth above (with credit for time served in international and domestic custody), order restitution in the amount of $2,500,000 (apportioned as set forth in the presentence report), and impose the mandatory $200 special assessment.

As set forth in its stipulated motion (Dkt. #53), the United States further requests that the Court order Defendant to forfeit a sum of money in the amount of $75,000 and various digital devices.

DATED this 17th day of June, 2021.

Respectfully submitted,

TESSA M. GORMAN
Acting United States Attorney

/s/ Steven Masada
STEVEN MASADA
FRANCIS FRANZE-NAKAMURA
Assistant United States Attorneys
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Telephone: 206.553.7970
Fax: 206.553.4440

ANTHONY TEELUCKSINGH
Senior Trial Attorney
Computer Crime and Intellectual Property Section, U.S. Department of Justice